UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,064	08/22/2003	Paul Moroney	018926-010110US	9712

7590 02/16/2007

Robert P. Marley
Motorola, Inc.
Broadband Communications Sector
101 Tournament Drive
Horsham, PA 19044

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/647,064	MORONEY ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12 April 2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed on 22 August 2003, with acknowledgement of priority date of 23 August 2002, based on provisional application filing of 60/405,537.

2. Claims 1-29 are currently pending in this application. Claims 1, 13, and 23 are independent claims.

3. The IDS submitted 12 April 2004 has been considered.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-29,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore U.S. Patent 6,697,489 (hereinafter '489) in view of Candelore et al. US Patent Application Publication No. 2003/0188162 (hereinafter '162).

As to independent claim 13, "A method for protecting interchip content pathways transporting digital content objects within a content processing unit, the method comprising steps of: loading a first key into a first key storage register in a first chip package, wherein the first key in the first key storage register is non-readable from outside the first chip package" is taught in '489 col. 5, lines 63-65, note the first chip package is interpreted equivalent to the smart card;

"encrypting digital content with the first key to produce ciphertext content" is disclosed in col. 7, lines 11-14, note the first key, is the unique key which is also in the unit, (set top box or equivalent conditional access system), the ciphertext content produced by the smart card is the encrypted CW, smart cards are non-readable from outside;

"coupling the ciphertext content from the first chip package to a content pathway; loading a second key into a second key storage register in a second chip package, wherein the second key in the second key storage register is non-readable from outside the second chip package; coupling the ciphertext content from the content pathway to a second chip package; and decrypting the ciphertext content with the second key to reformulate the digital conten" is shown in '489 col. 7, lines 30-36, the decryption engine uses the CW, i.e. the second key to produce plaintext content;

the following is not explicitly taught in '489: **"activating a feature of the first chip package that prevents overwriting the first key in the first key storage register from outside the first chip package"** however '162 teaches on page 2, paragraph 0030 "FIG. 3a illustrates a diagram of one embodiment of a configuration protocol for a lockable hard drive 105. At unit creation time, a configuration host 340 sends a status command to the hard drive 105 when the hard drive 105 powers up. The hard drive 105 sends a status acknowledgement that contains a bit that flags whether or not the hard drive 105 has been "locked". If the hard drive 105 is unlocked, the power-up status is sent as "un-locked" to the configuration host 340. In response, the configuration host 340 sends a lock command including a first key that is then stored in the hard drive's memory. The hard drive 105 then sets the "lock" bit, preventing a re-loading of the first

key in the hard drive. The hard drive 105 sends a lock acknowlement to the configuration host 340".

It would have been obvious to one of ordinary skill in the art at the time of the invention a method of securing Control Words (CWs) taught in '489 to include a means locking the unit to prevent over-writing of keys. One of ordinary skill in the art would have been motivated to perform such a modification because a protection mechanisms is needed to prevent the removal processors in order to gain unauthorized use of digital content see '162 (page 1, paragraph 0005). "Since an increasing number of electronic devices are becoming hard drive enabled, many of these electronic devices are subsidized by service providers to lower the initial cost for a customer. A problem exists today where buyers are capitalizing on the subsidized appliances by removing the hard drive from the electronic device and using it elsewhere. Hard drives may be taken out of the electronic device, and used for other purposes that were not intended by the electronic device manufacturer or service provider. For example, a hard drive in a set-top box may be physically removed from the set-top box. Once removed, the hard drive may be utilized with any number of hosts, one being a personal computer. The user benefits by not having to buy an additional hard drive and saving money as a result". In addition at least one inventor of '489 and '162 are the same, and the inventions are directed to similar subject matter, protection of digital content and the use of set top boxes.

As to dependent claim 14, **"further comprising steps of: providing a key encryption key in the at least one of the first and second chip packages; and decrypting at least one of the first and second keys with the key encryption key, whereby the at least one of the first**

and second keys is protected with the key encryption key outside the first chip package" is shown in '489 col. 6, lines 26-44.

As to dependent claim 15, **"further comprising a step of overwriting the second key in the second key storage register from outside the second chip package"** is taught in '489 col. 7, lines 15-20 that the unique key can be changed with a EMM message in '489.

As to dependent claim 16, **"further comprising steps of: encrypting the digital content or a derivative thereof in the second chip package to produce second ciphertext content using the second key or another key that is a function of the second key, coupling the second ciphertext content to a second content pathway"** is shown in '489 col. 7, line 59 through col. 8, line 19.

As to dependent claim 17, **"further comprising steps of: coupling the second ciphertext content from the second content pathway to a third chip package; and decrypting the second ciphertext content with the third key to reformulate the digital content"** is disclosed in '489 col. 7, line 59 through col. 8, line 19.

As to dependent claim 18, **"wherein: the content processing unit is part of a larger system comprising a plurality of functionally equivalent content processing units, and each of the plurality uses a different first key to protect their respective content pathways"** is disclosed in '489 teaches that the unique keys can be programmed during manufacture of the set top, TV, or NRSS-B module and '489 teaches that the traditional smart card could be replaced with a headend in col. 7, lines 59-65, the headend can deliver service keys encrypted based on the unique of the IC descrambler, the larger system is the cable network.

As to dependent claim 19, **"further comprising steps of: replacing at least one of the first and second chip packages; querying a database for at least one of the first and second keys; and loading at least one first and second keys into its respective chip package"** is disclosed in '489 col. 8, lines 58-65.

As to dependent claim 20, "further comprising steps of: replacing at least one of the first and second chip packages; and activating a secure re-start feature to load at least one of the first and second keys into its respective chip package from another chip package" is taught in '489 col. 7, lines 15-20 that the unique key can be changed with a EMM message or with a new smart card.

As to dependent claims 21 and 22, these claims are directed to a computer system or computer readable medium adapted to perform the computer-implementable method of claim 13; therefore they are rejected along similar rationale.

As to independent claim 1, "A content processing unit for protecting interchip content pathways transporting digital content objects, the content processing unit comprising: a first chip package, wherein the first chip package comprises a first body" is taught in '489 col. 5, lines 63-65, note the first chip package is interpreted equivalent to the smart card;

"a first plurality of interconnects" '489 teaches a plurality of interconnects to the smart card, i.e. by inserting into the conditional access system, programmed by manufacture, in col. 5, lines 29-49;

"an encryption engine, and" is shown in '489 col. 5, lines 36-37, note a smart card contains a cryptographic processor, i.e. encryption engine;

"a first key storage register capable of storing a first key wherein: the first key is used by the encryption engine to produce ciphertext content, the first key storage register is non-readable from outside the first body" is disclosed in col. 7, lines 11-14, note the first key, is the unique key which is also in the unit, (set top box or equivalent conditional access system), the ciphertext content produced by the smart card is the encrypted CW, smart cards are non-readable from outside;

"a second chip package, wherein the second chip package comprises: a second body" and **"a decryption engine",** is taught in '489 col. 7, lines 1-4;

"a second plurality of interconnects" '489 teaches several different kinds of interconnect to the second package, i.e. the conditional access unit in col. 5, line 65 through col. 7, line 15;

"and a second key storage register capable of storing a second key, wherein: the second key is used by the decryption engine to produce plaintext content from the ciphertext content" is shown in '489 col. 7, lines 30-36, the decryption engine uses the CW, i.e. the second key to produce plaintext content;

"and the second key storage register is non-readable from outside the second body" is disclosed in '489 col. 6, lines 26-36;

"a content pathway coupling a first subset of the first plurality and a second subset of the second plurality, wherein the content pathway transports the digital content objects as the ciphertext content" '489 teaches utilizing the smart card to receive encrypted CW and saving this CW for later use in col. 7, line 59 through col. 8, line 7;

the following is not explicitly taught in '489: **"and the first key storage register cannot be overwritten after a programmability period"** however '162 teaches on page 2, paragraph 0030 "FIG. 3a illustrates a diagram of one embodiment of a configuration protocol for a lockable hard drive 105. At unit creation time, a configuration host 340 sends a status command to the hard drive 105 when the hard drive 105 powers up. The hard drive 105 sends a status acknowledgement that contains a bit that flags whether or not the hard drive 105 has been "locked". If the hard drive 105 is unlocked, the power-up status is sent as "un-locked" to the configuration host 340. In response, the configuration host 340 sends a lock command including a first key that is then stored in the hard drive's memory. The hard drive 105 then sets the "lock" bit, preventing a re-loading of the first key in the hard drive. The hard drive 105 sends a lock acknowlement to the configuration host 340";

It would have been obvious to one of ordinary skill in the art at the time of the invention a method of securing Control Words (CWs) taught in '489 to include a means locking the unit to prevent over-writing of keys. One of ordinary skill in the art would have been motivated to perform such a modification because a protection mechanisms is needed to prevent the removal processors in order to gain unauthorized use of digital content see '162 (page 1, paragraph 0005). "Since an increasing number of electronic devices are becoming hard drive enabled, many of these electronic devices are subsidized by service providers to lower the initial cost for a customer. A problem exists today where buyers are capitalizing on the subsidized appliances by removing the hard drive from the electronic device and using it elsewhere. Hard drives may be taken out of the electronic device, and used for other purposes that were not intended by the electronic device manufacturer or service provider. For example, a hard drive in a set-top box

may be physically removed from the set-top box. Once removed, the hard drive may be utilized with any number of hosts, one being a personal computer. The user benefits by not having to buy an additional hard drive and saving money as a result". In addition at least one inventor of '489 and '162 are the same, and the inventions are directed to similar subject matter, protection of digital content and the use of set top boxes.

As to dependent claim 2, "wherein the programmability period ends when a command is sent to the first plurality" is taught in '489 col. 7, lines 15-20 that the unique key can be changed with a EMM message in '489.

As to dependent claim 3, "wherein the command activates a fusable link" however '162 teaches in claim 15, on page 5 that the lock bit can be set by a fuse. The motivation to combine '162 and '489 is the same as stated above in claim 1.

As to dependent claim 4, **"wherein the programmability period ends after writing to the first key storage register"** is taught in '489 col. 7, lines 1-4.

As to dependent claim 5, **"wherein: the content processing unit is a set top box, and the first chip package is a conditional access chip"** is disclosed in '489 col. 7, lines 1-15.

As to dependent claim 6, "wherein at least one of the first and second chip packages comprises a plurality of semiconductor substrates" is taught in '489 col. 7, lines 1-15.

As to dependent claim 7, "wherein: at least one of the first and second chip packages further comprises a key encryption key, and at least one of the first and second keys is protected with the key encryption key outside the first body" is shown in '489 col. 6, lines 26-44.

As to dependent claim 8, **"wherein the second key storage register is overwritable by manipulating the second plurality"** '489 teaches that the CWs could only be valid for a certain period of time and that the register can store multiple keys, therefore it is obvious that the second key storage register would be over written.

As to dependent claim 9, "wherein: the second chip package further comprises a second encryption engine, and the second encryption engine uses the second key or another key that is a function of the second key to encrypt the content object or a derivative thereof" is shown in '489 col. 7, line 59 through col. 8, line 19.

As to dependent claim 10, "further comprising a third chip package comprising a third key that can decrypt ciphertext produced with the second encryption engine" is disclosed in '489 col. 7, line 59 through col. 8, line 19.

As to dependent claim 11, "wherein: the content processing unit is part of a larger system comprising a third plurality of functionally equivalent content processing units, and each of the third plurality uses a different first key to protect their respective content pathways" is disclosed in '489 teaches that the unique keys can be programmed during manufacture of the set top, TV, or NRSS-B module and '489 teaches that the traditional smart card could be replaced with a headend in col. 7, lines 59-65, the headend can deliver service keys encrypted based on the unique of the IC descrambler, the larger system is the cable network.

As to dependent claim 12, "wherein the digital content objects are either compressed or non-compressed" is taught in '489 col. 8, lines 50-58.

As to independent claim 23, this claim contains substantially similar subject matter as independent claim 1; therefore it is rejected along the same rationale. The Examiner interprets

"the first key storage cannot be overwritten after being written once" equivalent to "the first key storage cannot be overwritten after a programmability period". Since in claim 23 the period is zero.

As to dependent claim 24, **"wherein: the first key storage register has a third plurality of bits, and each of the third plurality can only change its stored value, at most, one time"** however '162 teaches "In one embodiment, the lock bit is written to one time programmable (OTP) memory and not changeable. In alternative embodiments, the lock bit may be re-programmable. Under the right conditions, the use of a master key may be used to revert the hard drive to an un-locked condition" on page 3, paragraph 0040.

As to dependent claim 25, "wherein: at least one of the first and second chip packages further comprises a key encryption key, and at least one of the first and second keys is protected with the key encryption key outside the first body" is taught in '489 col. 5, lines 29-32 and col. 6, lines 16-36.

As to dependent claim 26-29, these claims contain substantially similar subject matter as claims 8-11; therefore they are rejected along similar rationale.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
12 February 2007